Let's Encrypt証明書取得 クイックセットアップ 2019年版

2019/01/08
Ports や pkg にある py-certbot を使って証明書取得できたのでメモ書き。

導入パッケージ

py36-certbot と py27-certbot の二つがあるpkgからでもPortsからでも導入可能。
ただ、ウチの環境ではpy36-certbot は動作しなかったので py27-certbotを使う。

証明書取得

先にDNSで正引き可能なドメインを取得してサーバを稼働させておく必要がある。
またcertbotを実行させる前に80番ポートを使うサービスは止めておくこと。

この例ではmimiqrr.dip.jp 用の証明書を取得している。

```
root@www:~ # certbot certonly --standalone -d mimiqrr.dip.jp -m
k896951@gmail.com
Saving debug log to /var/log/letsencrypt/letsencrypt.log
Plugins selected: Authenticator standalone, Installer None

- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
- -
Please read the Terms of Service at
https://letsencrypt.org/documents/LE-SA-v1.2-November-15-2017.pdf. You must
agree in order to register with the ACME server at
https://acme-v02.api.letsencrypt.org/directory
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
- -
(A)gree/(C)ancel: A←Aを入力

- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
- -
Would you be willing to share your email address with the Electronic
Frontier
Foundation, a founding partner of the Let's Encrypt project and the non-
profit
organization that develops Certbot? We'd like to send you email about our
work
encrypting the web, EFF news, campaigns, and ways to support digital
freedom.
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
- -
```

```
(Y)es/(N)o: Y□□□←Yを入力
Obtaining a new certificate
Performing the following challenges:
http-01 challenge for mimiqrr.dip.jp
Waiting for verification...
Cleaning up challenges

IMPORTANT NOTES:
 - Congratulations! Your certificate and chain have been saved at:
   /usr/local/etc/letsencrypt/live/mimiqrr.dip.jp/fullchain.pem
   Your key file has been saved at:
   /usr/local/etc/letsencrypt/live/mimiqrr.dip.jp/privkey.pem
   Your cert will expire on 2019-04-05. To obtain a new or tweaked
   version of this certificate in the future, simply run certbot
   again. To non-interactively renew *all* of your certificates, run
   "certbot renew"
 - Your account credentials have been saved in your Certbot
   configuration directory at /usr/local/etc/letsencrypt. You should
   make a secure backup of this folder now. This configuration
   directory will also contain certificates and private keys obtained
   by Certbot so making regular backups of this folder is ideal.
 - If you like Certbot, please consider supporting our work by:

   Donating to ISRG / Let's Encrypt:   https://letsencrypt.org/donate
   Donating to EFF:                    https://eff.org/donate-le

root@www:~ #
```

表示に従い、/usr/local/etc/letsencrypt を確認してみる。

```
root@www:~ # ls -l /usr/local/etc/letsencrypt/
total 28
drwx------  3 root  wheel  512  1月 6 04:09 accounts
drwx------  3 root  wheel  512  1月 6 04:10 archive
drwxr-xr-x  2 root  wheel  512  1月 6 04:10 csr
drwx------  2 root  wheel  512  1月 6 04:10 keys
drwx------  3 root  wheel  512  1月 6 04:10 live
drwxr-xr-x  2 root  wheel  512  1月 6 04:10 renewal
drwxr-xr-x  5 root  wheel  512  1月 6 04:09 renewal-hooks
root@www:~ # ls -l /usr/local/etc/letsencrypt/csr
total 4
-rw-r--r--  1 root  wheel  924  1月 6 04:10 0000_csr-certbot.pem
root@www:~ # ls -l /usr/local/etc/letsencrypt/live
total 8
-rw-r--r--  1 root  wheel  740  1月 6 04:10 README
drwxr-xr-x  2 root  wheel  512  1月 6 04:10 mimiqrr.dip.jp
root@www:~ # ls -l /usr/local/etc/letsencrypt/live/mimiqrr.dip.jp
total 4
lrwxr-xr-x  1 root  wheel   39  1月 6 04:10 cert.pem ->
../../archive/mimiqrr.dip.jp/cert1.pem
lrwxr-xr-x  1 root  wheel   40  1月 6 04:10 chain.pem ->
```

```
../../archive/mimiqrr.dip.jp/chain1.pem
lrwxr-xr-x  1 root  wheel   44  1月 6 04:10 fullchain.pem ->
../../archive/mimiqrr.dip.jp/fullchain1.pem
lrwxr-xr-x  1 root  wheel   42  1月 6 04:10 privkey.pem ->
../../archive/mimiqrr.dip.jp/privkey1.pem
-rw-r--r--  1 root  wheel  692  1月 6 04:10 README
root@www:~ #
```

無事 /usr/local/etc/letsencrypt/live/mimiqrr.dip.jp に証明書が格納された。 実体へシンボリックリンクで、実体は更新が行われるたび末尾の数値が増えていく。

証明書更新

まだ更新時期じゃない場合はこんなメッセージが表示される。

```
root@www:/ # certbot renew
Saving debug log to /var/log/letsencrypt/letsencrypt.log

- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
- -
Processing /usr/local/etc/letsencrypt/renewal/mimiqrr.dip.jp.conf
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
- -
Cert not yet due for renewal

- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
- -

The following certs are not due for renewal yet:
  /usr/local/etc/letsencrypt/live/mimiqrr.dip.jp/fullchain.pem expires on
2019-04-06 (skipped)
No renewals were attempted.
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
- -
root@www:/ #
```

オプションに“ –force-renewal”を付与すると期限に関係なく更新できる。この例だと、3回目の更新になる。

```
root@www:/ # certbot renew --force-renewal
Saving debug log to /var/log/letsencrypt/letsencrypt.log

- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
- -
Processing /usr/local/etc/letsencrypt/renewal/mimiqrr.dip.jp.conf
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
- -
Plugins selected: Authenticator standalone, Installer None
Renewing an existing certificate
```

```
Performing the following challenges:
http-01 challenge for mimiqrr.dip.jp
Waiting for verification...
Cleaning up challenges

- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
- -
new certificate deployed without reload, fullchain is
/usr/local/etc/letsencrypt/live/mimiqrr.dip.jp/fullchain.pem
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
- -

- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
- -

Congratulations, all renewals succeeded. The following certs have been
renewed:
  /usr/local/etc/letsencrypt/live/mimiqrr.dip.jp/fullchain.pem (success)
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
- -
root@www:/ # ls -l  /usr/local/etc/letsencrypt/live/mimiqrr.dip.jp/
total 4
lrwxr-xr-x  1 root  wheel   39  1月  8 02:12 cert.pem ->
../../archive/mimiqrr.dip.jp/cert3.pem
lrwxr-xr-x  1 root  wheel   40  1月  8 02:12 chain.pem ->
../../archive/mimiqrr.dip.jp/chain3.pem
lrwxr-xr-x  1 root  wheel   44  1月  8 02:12 fullchain.pem ->
../../archive/mimiqrr.dip.jp/fullchain3.pem
lrwxr-xr-x  1 root  wheel   42  1月  8 02:12 privkey.pem ->
../../archive/mimiqrr.dip.jp/privkey3.pem
-rw-r--r--  1 root  wheel  692  1月  6 04:10 README
root@www:/ #
```

技術資料, www, Apache, SSL, Let'sEncrypt

From:
https://wiki.hgotoh.jp/ - **努力したWiki**

Permanent link:
https://wiki.hgotoh.jp/documents/quick/quick-0023

Last update: **2023/04/14 02:32**